UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/816,869	03/24/2001	C. Andrew Neff	324628002US3	6077

25096 7590 10/20/2004

PERKINS COIE LLP
PATENT-SEA
P.O. BOX 1247
SEATTLE, WA 98111-1247

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/816,869	NEFF, C. ANDREW	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/01 thru 8/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: original application filed 24 March 2001, with acknowledgement of continuing data filing date of 24 March 2000.

2. Claims 1-35 are currently pending in this application. Claims 1, 6, 10, 18, 28, and 35 are independent claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

4. **Claims 6, 9-18, 26, 27, 28, and 30-35** are rejected under 35 U.S.C. 102(e) as being anticipated by Challenger et al. U.S. Patent No. 6,081,793 (hereinafter '793).

As to independent claim 6, "A computer system for receiving a sequence of elements, comprising: a server computer coupled to a computer network and configured to:" is taught in '793 col. 1, lines 54-60;

"receive a sequence of electronic data elements representing individual data files" is shown in '793 col. 3, lines 39-50;

"apply a cryptographic transformation using at least a first secret key to anonymously permute the sequence of electronic data elements and produce a first shuffled sequence of electronic data elements, wherein the server computer knows a correspondence

between the first shuffled sequence of electronic data elements and the sequence of electronic data elements, and" is disclosed in '793 col. 3, line 66 through col. 4, line 15;

"generate a first linear size proof of correctness for the first shuffled sequence of electronic data elements based on a scaled iterated logarithmic multiplication proof" is shown in '793 col. 10 ,lines 14-24.

As to dependent claim 9, "wherein the sequence of electronic elements are public keys" is disclosed in '793 col. 3, lines 10-15;

"and wherein the server if further configured to check, in response to a request from an individual, that the individual has a value uniquely and mathematically related to a one of the public keys" is taught in '793 col 3, lines 60-63;

"and if so, issue a certificate to the one individual" is shown in '793 col.6, lines 45-64.

As to independent claim 10, "A computer-implemented method, comprising: receiving a plurality of public keys from a corresponding plurality of individuals, wherein each of the plurality of individuals have a private key corresponding to one of the plurality of public keys" is shown in '793 col. 3, lines 11-28;

"receiving a request for a certificate from one of the plurality of individuals having a one private key; providing at least a subset of the plurality of public keys to the requesting individual; receiving a shuffle of the plurality of public keys and a linear size proof of correctness for the shuffled public keys based on a scaled iterated logarithmic multiplication proof and a value corresponding to the one private key" is disclosed in '793 col. 3, line 66 through col. 4, line 15;

"wherein the value provides proof that the one individual has knowledge of the one private key without revealing the one private key; checking the proof of correctness; checking that the value is mathematically related to a one of the public keys that corresponds to the one private key; issuing a certificate to the one individual; and reducing the plurality of public keys by the one public key" is taught in '793 col. 10, lines 14-24.

As to dependent claim 11. The method of claim 10 wherein the method further includes setting a value G to a subgroup operator g from an Z_p or elliptic curve group, wherein providing at least a subset of the plurality of public keys includes providing all of the then current public keys H" is shown in '793 col. 3, line 66 through col. 4, line 15.

As to dependent claim 12, " wherein providing at least a subset of the plurality of public keys includes providing at least a subset of a plurality of public key pairs, wherein receiving a shuffle of the plurality of public keys includes receiving a shuffle of a true subset of the plurality of public key pairs as selected by the one individual" is disclosed in '793 col. 8, lines 19-34.

As to dependent claim 13, "further comprising: receiving from each of a plurality of authorities, in sequence, a shuffled set of the plurality of public keys H' based on a secret cryptographic shuffle operation performed on at least a subset of the plurality of public keys to produce the shuffled set of the plurality of public keys H'; receiving from each of a plurality of authorities, in sequence, a verification transcript of the cryptographic shuffle operation; and verifying a correctness of the cryptographic shuffle operation based on the verification transcript; and if verified, then setting at least a subset of the plurality of public keys to H to H'" is taught in '793 col. 8, lines 37—50.

As to dependent claim 14, "further comprising: at a time after receiving at least some of the plurality of public keys, setting at least a subset of the then received plurality of public keys to a received shuffled set of the plurality of public keys, wherein the shuffled set of the plurality of public keys have been received from a third party" is shown in '793 col. 3, lines 2-29.

As to dependent claim 15, "further comprising: receiving the issued certificate from the one of the plurality of individuals; and providing an electronic ballot to the one individual" is disclosed in '793 col. 3, lines 45-50.

As to dependent claim 16, "wherein issuing a certificate includes digitally signing the received request to produce a public key infrastructure ("PKI") certificate" is taught in '793 col. 6, lines 50-55.

As to dependent claim 17, "further comprising: receiving issued certificates from at least some of the plurality of individuals and providing initial electronic ballots in response thereto; and receiving unencrypted voted ballots from the at least some of the plurality of individuals" is shown in '793 col. 7, lines 19-33.

As to independent claim 18, "A computer-implemented cryptographic method between a prover computer and a verifier computer, the method comprising: selecting a subgroup generator g selected from a group G; secretly generating a prover key c, and a commitment value C based on the subgroup generator g; secretly establishing a cryptographic relationship between first and second sequences of elements; providing to the verifier computer the commitment C and the first and second sequences of elements,

but not the cryptographic relationship; computing a series of proof values based on the cryptographic relationship; and" is disclosed in '793 col. 3, lines 36-60;

"providing the series of computed proof values to the verifier computer as a non-interactive proof of knowledge that the prover computer has access to the cryptographic relationship without revealing the cryptographic relationship to the verifier computer" is taught in '793 col. 6, lines 50-55.

As to dependent claim 26, "wherein the group G is Z_p" is shown in '793 col. 3, line 66 through col. 4, line 15.

As to dependent claim 27, "wherein the group G is an elliptic curve group" is disclosed in '793 col. 3, line 66 through col. 4, line 15.

As to independent claim 28, this claim is directed to a computer-readable medium of the system of claim 6 and therefore is rejected along similar rationale.

As to dependent claim 30, "wherein the computer-readable medium is a logical node in a computer network receiving the sequence of electronic data elements and the contents" is taught in '793 col. 3, lines 39-50.

As to dependent claim 31, this claim is directed to a computer-readable medium of claim 28 and is rejected along the same rationale.

As to dependent claim 32, this claim is directed to a data transmission medium of claim 28 and is rejected along the same rationale.

As to dependent claim 33, this claim is directed to a computer-readable medium of claim 28 and is rejected along the same rationale.

As to dependent claim 34, "wherein the computer-readable medium is an Internet connection link to a voting authority server computer" is taught in '793 col. 7, line 53-58.

As to independent claim 35, this claim is substantially similar to claim 6 and is rejected along the same rationale.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-4, 7, 8, 19-25, and 29,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '793 in further view of Kilian et al. U.S. Patent No. 5,682,430 (hereinafter '430).

As to dependent claim 1, "An electronic voting system for use with a computerized network, comprising: a plurality of voting computers coupled to the computerized network" is taught in '793 col. 1, lines 54-60 "It is one objective of the present intention to provide an improved method and system for voting ... as well as electronic voting utilizing the internet";

"wherein each voting computer provides an electronic encrypted ballot, wherein each electronic ballot is encrypted under a discrete log asymmetric encryption process using underlying groups Z_p or elliptic curve" is shown in '793 col. 3, line 66 through col. 4, line 15 "one or more cryptographic operations are utilized to encrypt data flows between the

voter (and his or her smart card and /or personal computer), and the authentication servers, the journal servers, and the results servers";

"at least first, second and third authority computers coupled to the computerized network" is disclosed in '793 col. 3, line 36-38 "three separate data processing servers collaborate in order to maximize security and privacy throughout the voting process";

"wherein the first authority computer is configured to receive a series of electronic ballots corresponding to an aggregation of each of the electronic ballots received from the plurality of voting computers" is taught in '793 col. 3, lines 39-50 "One or more authentication servers are identified to particular electronic precincts and conventional precincts ";

"and to apply a secret, one-way cryptographic transformation using at least a first secret key to anonymously shuffle the series of electronic ballots and produce a first shuffled series of ballots, wherein only the first authority computer knows a correspondence between the first series of shuffled ballots and the series of electronic ballots, and wherein the first authority computer is further configured to provide a first linear size, non-interactive proof of correctness for the first series of shuffled ballots based on a scaled iterated logarithmic multiplication proof" is shown in '793 col. 10 , lines 14-24 "The entire package is sent to the authenticator the public key of the voter "VX," but the authentication cannot read the actual competed vote, thus ensuring privacy of the voting choices, since it is encrypted with the ballot counter's public key"

"wherein the second authority computer is configured to receive the first series of shuffled ballots, to apply the cryptographic transformation using at least a second secret key to anonymously shuffle the first series of shuffled ballots and produce a second series of

shuffled ballots" is disclosed in '793 col. 3, lines 49-59 "A journal server is also provided. In practice, many journal servers may be provided each journal server being identified with one or more particular authentication servers";

"wherein only the second authority computer knows a correspondence between the first series of shuffled ballots and the second series of shuffled ballots, and wherein the second authority computer is further configured to provide a second linear size, non-interactive proof of correctness for the second series of shuffled ballots based on the scaled iterated logarithmic multiplication proof" is shown in '793 col. 8, lines 19-38 "The journal server examine the cryptolope, in accordance with block 405. In accordance with block 407, the journal server determines whether the cryptolope has been tampered with";

"wherein the third authority computer is configured to receive the second series of shuffled ballots, to apply the cryptographic transformation using at least a third secret key to anonymously shuffle the second series of shuffled ballots and produce a third series of shuffled ballots, wherein only the third authority computer knows a correspondence between the third series of shuffled ballots and the second series of shuffled ballots, and wherein the third authority computer is further configured to provide a third linear size, non-interactive proof of correctness for the third series of shuffled ballots based on the scaled iterated logarithmic multiplication proof" is disclosed in '793 col. 8, lines 38-53 "The results server then examines the cryptolope in accordance with block 425. In accordance with block 427, determination is made as whether the cryptolope has been tampered with ... is added to the election results by the results server";

the following is not taught in '793: **"and a verification computer coupled to the computerized network, wherein the verification computer is configured to receive the proofs of correctness from the first, second and third authority computers and without interacting with the first, second and third authority computers, to verify a correctness of the shuffled ballots"** however '430 teaches "A three-step procedure is followed by each mixing center ... Also, the invention results in a method which reduces the amount of communication and computation necessary to generate, transmit and check the proofs by combining multiple proofs into a single proof" in col. 2, lines 8-30.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '793 an electronic voting system to include a means to perform verification without interacting with the first, second and third authority computers. One of ordinary skill in the art would have been motivated to perform such a modification because there is no means for an observer to verify the results of an election. As indicated by '430 (see col. 1, lines 35 et seq.) "There is usually no way for an outside observer to later verify that the election was properly performed".

As to dependent claim 2, "further comprising: a server computer system coupled to the computerized network, wherein the server computer system is configured to: receive the plurality of electronic ballots from the plurality of voting computers; verify a proof of validity of each of the plurality of electronic ballots; form an encrypted tally of the votes from the plurality of electronic ballots; transmit the encrypted tally to the first, second and third authority computers; receive ballot decryption shares produced from at least two of the first, second and third authority computers; and compute a decrypted tally;

and at least one voting poll computer coupled to the computerized network and providing some of the plurality of electronic encrypted ballots to the server computer system" is taught in '793 col. 10, lines 6-13 "The entire package is sent to the authenticator. The authenticator verifies the vote is from the voter ... both the authenticator cannot read the actual completed both, thus ensuring privacy of the voting choices".

As to dependent claim 3, "wherein the first, second and third authority computers are configured to provide Chaum-Pedersen proofs for the first, second and third shuffles of the ballots, respectively, and wherein each of the first, second and third authority computers generate an initial challenge series, receive a challenge from at least one verification computer, and generate the cryptographic transformation based on an exponentiation of the initial and received challenges" is shown in '430 col. 4, lines 33-64 "calculates the following values using the secret key x_i ... showing that H is generated in this manner from G".

As to dependent claim 4, "wherein the computerized network includes the World Wide Web, wherein each of the plurality of voting computers and first ... authority computers include a web browser program" is disclosed in 793 col. 7, line 53-58 "wherein the data processing system operating as the "internet client";

"second" is taught in '793 col. 4, lines 57-58 "that a plurality of Intelligent Work Stations (IWS) coupled to a host process may be utilized for each such network. Any of the processin gsystem may also be connected to the internet as shown";

"and third" is shown in '793 col. 6, lines 56-59 "a distributed data processing system and/or the internet"".

As to dependent claim 7, "wherein the received sequence of electronic data elements are encrypted using Z_p or elliptic curve groups using a key unknown to the server computer, and wherein the server computer is further configured to: receive a series of randomly generated values e_i from a verifier computer; secretly generate a series of values U_i based on a secret, one-way cryptographic transformation that employs the received series of values e_i and secretly generated values U_i permute the sequence of electronic data elements to produce the first shuffled sequence of elements based on the series of values U_i and a secret value d" is disclosed in '793 col. 10, lines 14-24;

"and provide the values U_i and a series of proof values based on the cryptographic transformation as a proof of knowledge that the server computer has access to how the cryptographic transformation permuted the sequence of electronic data elements to produce the first shuffled sequence of elements" is taught in '793 col. 3, lines 49-59;

"without revealing the cryptographic transformation to the verifier computer" is shown in '430 col. 2, lines 8-30 "".

As to dependent claim 8, "wherein the server computer is further configured for: receiving a plurality of public keys from a corresponding plurality of individuals, wherein each of the plurality of individuals have a private key corresponding to one of the plurality of public keys; receiving a request for a certificate from one of the plurality of individuals having a one private key; providing at least a subset of the plurality of public keys to the requesting individual" is disclosed in '793 col. 3, lines 10-15 "The information contained on each smart card is depicted in block diagram for in FIG. 2A. As is shown , smart

card 219 includes the voter identification , the public key associated with that voter identification, a private key"

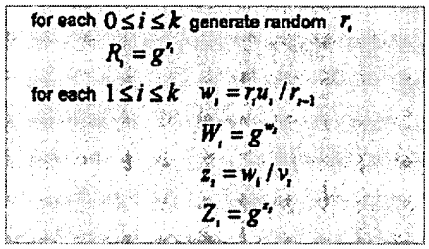
"receiving a shuffle of the plurality of public keys and a linear size proof of correctness for the shuffled public keys based on a scaled iterated logarithmic multiplication proof and a value corresponding to the one private key, wherein the value provides proof that the one individual has knowledge of the one private key without revealing the one private key" is shown in '430 col. 2, lines 8-30;

"checking the proof of correctness; checking that the value is mathematically related to a one of the public keys that corresponds to the one private key; issuing a certificate to the one individual; and reducing the plurality of public keys by the one public key" is disclosed in '793 col. 3, lines 11-28.

As to dependent claim 19. The method of claim 18 wherein at least the second sequence of elements is a sequence of encrypted ballots, wherein each ballot is encrypted using Z_p or elliptic curve groups; wherein the first and second sequences of elements are respectively $(X_1, \ldots, X_k)$ and $(Y_1, \ldots, Y_k)$ wherein the first and second sequence of elements have the cryptographic relationship and wherein computing and providing the series of proof

$$(g^{n_1},\ldots,g^{n_k}) = (X_1,\ldots,X_k)$$
$$(g^{r_1},\ldots,g^{r_k}) = (Y_1,\ldots,Y_k) \text{ and where}$$
$$c^k \prod_{i=1}^{k} u_i = \prod_{i=1}^{k} v_i$$

values includes providing Chaum-Pedersen proofs based on:



wherein the Chaum-Pedersen proofs provided to the verifier computer are of a form:

is taught in '430 col. 3, lines 20-40 "For ease of explanation, the three steps of decrypt, shuffle and prove of the centers will be described in this order … is posted, permuted with the other processed messages for use by the mixing center".

As to dependent claim 20, "further comprising: permuting the first sequence of elements to produce the second sequence of elements based on a cryptographic transformation; receiving a randomly generated value t from the verifier computer; secretly generating a value T based on the received value t and the subgroup generator, and secretly generating a value S based on the received value t and the prover key c; and wherein computing and providing to the verifier computer the series of proof values includes providing a series of values based on the cryptographic transformation as a proof of knowledge that the prover computer has access to how the cryptographic transformation permuted the first sequence of elements to produce the second sequence of elements without revealing the cryptographic transformation to the verifier computer" is shown in '430 col. 3, line 55 through col. 4, line 50 "The algorithm prove-DECRYPT and

prove-SHUFFLE will now be described ... The proof comprises, given (A, B, g, w) showing that B could be generated in this manner from A".

As to dependent claim 21, "further comprising: permuting the first sequence of elements to produce the second sequence of elements based on a cryptographic transformation in a form of

$$(g^{\alpha_1},\ldots,g^{\alpha_k}) = (X_1,\ldots,X_k)$$
$$(g^{\alpha_{\pi(1)}},\ldots,g^{\alpha_{\pi(k)}}) = (Y_1,\ldots,Y_k)$$

receiving a randomly generated value t from the verifier computer; secretly generating a value T based on raising the subgroup generator g to the received value t, and secretly generating a value S based on raising the value T to the prover key c; and wherein computing and providing to the verifier computer the series of proof values includes providing a series of values based on the cryptographic transformation in a form of:

$$U_i = X_i / T$$
$$V_i = Y_i / S$$

as a proof of knowledge that the prover computer has access to how the cryptographic transformation permuted the first sequence of element to provide the second sequence of elements without revealing the cryptographic transformation to the verifier computer" is disclosed in '430 col. 5, lines 3-49 "While these algorithms are given in terms of a verifier, a more efficient solution is to use the Fiat-Shamir method of eliminating interaction ... Similarly, as a variation of the above scheme".

As to dependent claim 22, "further comprising: receiving the first sequence of elements as a set of elements that have previously been permuted in a manner unknown to the prover computer; receiving a series of randomly generated values e_i from the verifier computer; secretly generating a series of values U_i based on a secret cryptographic transformation that employs the received series of values e_i and secretly generated values U_i permuting the second sequence of elements with respect to the first sequence of elements based on the series of values U_i and a secret value d; and wherein computing and providing to the verifier computer the series of proof values includes providing the resulting values U_i and providing a series of proof values based on the cryptographic transformation as a proof of knowledge that the prover computer has access to how the cryptographic transformation permuted the first sequence of element to provide the second sequence of elements without revealing the cryptographic transformation to the verifier computer" is taught in '430 col. 3, lines 40-53.

As to dependent claim 23, "further comprising: receiving the first sequence of elements as a set of elements that have previously been permuted in a manner unknown to the prover computer; receiving a series of randomly generated values e_i from the verifier computer; secretly generating a series of values U_i based on a secret cryptographic transformation of a form

$$u_i = \bar{u}_i + e_i = \log_g U_i$$

permuting the second sequence of elements with respect to the first sequence of elements based on the series of values U_i and a secret value d based on the following operations

$$(V_1,\ldots,V_k)=(U^d_{\pi(1)},\ldots,U^d_{\pi(k)})$$
$$D=g^d$$
$$v_i=\log_g V_i$$
$$A_i=X_i^{v_i}$$
$$B_i=Y_i^{v_i}$$

and wherein computing and providing to the verifier the series of proof values includes providing the resulting values U_i

$$A=\prod_{i=1}^{k} A_i$$
$$B=\prod_{i=1}^{k} B_i$$

and for $1 \preceq i \succeq k$, providing a series of proof Chaum-Pedersen of a form

$$(g,V_i,X_i,A_i) \text{ and } (g,U_i,Y_i,B_i)$$

and a Chaum-Pedersen proof for (D, A, C, B) as a proof of knowledge that the prover computer has access to how the cryptographic transformation permuted the first sequence of element to provide the second sequence of elements without revealing the cryptographic transformation to the verifier computer" is shown in '430 col. 3, lines 40-53.

As to dependent claim 24, "further comprising repeating the receiving the first sequence of elements, receiving a series of randomly generated values, secretly generating a series of values, and permuting the second sequence of elements for l-tuple of elements in the first sequence of elements" is disclosed in '430 col. 4, lines 25-40 "the second step comprises generating r_1, r_2, ... and a permutation Π and generating a set of pairs".

As to dependent claim 25, "wherein receiving the first sequence of elements includes receiving a subset of a set of identifying elements, wherein each identifying element in the set corresponds to an individual, and wherein the method further comprises: receiving an

anonymous certificate if the verifying computer verifies the series of proofs" is shown in '430 col. 5, lines 5-25 "While these algorithms are given in terms of a verifier, a more efficient solution .... It is necessary to show that the following equation holds for each pair".

As to dependent claim 29. The computer-readable medium of claim 28 wherein the received sequence of electronic data elements are encrypted with an underlying mathematical group being a ring of integers having a modulus integer value p (Z_p)" is disclosed in '430 col. 4, lines 20-45 "In order to describe the algorithm prove-SHUFFLE, the second step is abstracted as follows ... The prover uniformly chooses $t \in Z_{p-1}$, random permutation".

7. **Claim 5** is rejected under 35 U.S.C. 103(a) as being unpatentable over '793 in further view of '430 in further view of Davis et al. U.S. Patent No. 6,550,675 (hereinafter '675).

As to dependent claim 5, the following is not taught in the combination of '793 and '430 **"wherein the plurality of voter computers include at least one palm-sized computer, cell phone, wearable computer, interactive television terminal or Internet appliance"** however '675 teaches "It is further object of the invention to provide a voting system that is easy to use, has a portable Voting Machine" in col. 1, lines 26-30.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of teachings of '793 and '430 an electronic voting system with a means to perform verification to include the ability to have portable voter computers. One of ordinary skill in the art would have been motivated to perform such a modification to facilitate voting. As indicated by '675 (see col. 1, lines 15 et seq.) "Voting systems have generally been

developed to facilitate voting. However, these systems are not highly reliable and are not flexible for use in a variety of voting conditions".

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. "**After 26 October 2004, the examiner can be reached at (571) 272-3842".** The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
7 October 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100